Blockchain Assignment

gvch48

Task 1.1

User ID: gvch48

Block Hash Target: 0x000003e7fc180000000000000000000000000000000000000000000000000000

Nonce: 287772

Hashes required: 287773

Time taken (seconds): 6.327823162078857

Time per hash (seconds): 2.198893976182219e-05

$$Expected\ \#Hashes = \frac{difficulty\ \times\ 2^{256}}{0xffff\ \times\ 2^{208}}\ =\ (difficulty\ \times\ 2^{48})/0xffff$$

$$Estimated\ Time\ To\ Mine\ \ = Time\ per\ hash\ \times Expected\ \#Hashes$$

Estimated Time to Mine Valid Block on my PC at Difficulty = 1:
93861.85514882216 seconds ≈ 26 years

Estimated Time to Mine Valid Block on my PC at Difficulty = 7,454,968,648,263:
6.997371874022747e+17 seconds ≈ 22,000,000,000 years

Task 1.2

ECDSA public (verifying) key:
324c3af2029a6b5e071c93b427755a44a10033691e2a4ff4b140ad4d74cdee5241ec5dd9a3b510c46de
009aeee9ac7bdc82ff33f61d6bd78601321691419ffbd

Signature of ‘Hello world’:
99799954427902f68cb535e28f3d81e4771dddc7b25edbe4c305d32e48afb58a6c1b8767b57241160e
fe8a51bcea83eeba005f2e751cf069406f4f053720c78b

Signature of Previous Block:
bb05109bf26b7076c980ae1e84d084d4f8a43b10c082d85321da3c00e25c1380e92bf6d1141eab0e27
46b2653dc8c37685694a394bff9f2bb3cee29d871580aa

8 bytes = 16 Hexadecimal digits, so the first 16 digits of the hexadecimal representation of the hash of the signature of the previous block is my hit value

Hit Value: 44290d165d5f5ec8

$$Time\ to\ Mine\ (seconds) = \frac{Hit\ Value}{Base\ Target\ \times Effective\ Balance}$$

My Time to Mine (seconds): 83.20355950598146

Task 2

User ID: gvch48

Task 2.1

Transaction 1

https://www.blockchain.com/btc/tx/d01fe0285810688e49a26b3f047035aab039d9d061fb82f0af4ca0ac5e6e5183?show_adv=true

A standard transaction with funds from 3 addresses going to another address, with 0.001BTC being the likely payment amount, and the other output being a change address. It is likely that the inputs are all owned by one person.

Transaction 2

https://www.blockchain.com/btc/tx/6074e560633a3046c07cbc97d2644150138e8e0bee6eb77e3b354ba8aafee128

This is another standard transaction, except that this one uses SegWit, so the input script has a ScriptSig and a Witness

Transaction 3

https://www.blockchain.com/btc/tx/23d18389ec5badfb357e0c81eb3d4f5899897709edcf24218754c25617122e61

One of the outputs is used to write Omni Protocol encoded data to the blockchain. Omni is a Protocol that allows altcoins that don’t have their own blockchain to run on top of the Bitcoin blockchain. This transaction was used to send Tether. You can view the transaction here: https://www.omniexplorer.info/search/23d18389ec5badfb357e0c81eb3d4f5899897709edcf24218754c25617122e61

Task 2.2

Bitcoin-testnet address: n4KqzBMw2tgTWJeib2AQGYBc2cqH3jyUx1

Transaction ID: 1171a5046723044f76f26a370729ccfeb5c9f7b77c4f95cd9c6518314d850cdd

https://chain.so/tx/BTCTEST/1171a5046723044f76f26a370729ccfeb5c9f7b77c4f95cd9c6518314d850cdd

Task 2.3

Transaction ID: 5c2c4a82afb4c1da696b37f3e6e8b54abed48bca137f709b00797ba33a9f3715

https://chain.so/tx/BTCTEST/5c2c4a82afb4c1da696b37f3e6e8b54abed48bca137f709b00797ba33a9f3715

Hex used as script: 6a4c06677663683438

I inspected the raw data of your example proof of burn transaction to find the script_asm and script_hex fields. I used a hex to ascii converter to verify that the second part of script_asm decodes to your message "Magnus rules the world!". I then assumed that the first 6 hex digits 6a4c17 were

Script OP Codes. I went to the list of script op codes and found that 6a was OP_RETURN and 4c was OP_PUSHDATA1. The description of OP_PUSHDATA1 told me that 17 must be the number of bytes to be pushed to the stack. I checked and 17 in hex is 23, and your message was 46 hex digits = 23 bytes long. I then converted gvch48 to hex and calculated its length in bytes. Then it was just a matter of putting it all back together.

Task 3

In deciding which asset to invest in, I have first made a few assumptions:

Assumptions:

- I am not investing ALL my money into this asset. Ease of spending is not a factor for investment since I assume I will still use fiat currencies for everyday purchases

- I assume I am willing to hold this investment for a long time, and am not interested in short timeframe fluctuations in price (unless there is a bubble and I can sell high fast before it bursts), but rather am more interested in long-term growth

- I assume that none of these assets will become easily tradable in everyday life any time soon, so will need to be sold for fiat currency to redeem its value

- I looked into how HMRC taxes gold and Cryptoassets, but it’s quite complicated so I’m not considering Taxes as a factor

Gold

The major advantage of investing in gold is its stability and reliability. It has been an asset with value for a lot of human history, and that isn’t likely to change. Also, while its price does fluctuate, the changes are over many years, so you’re not going to lose your wealth overnight. Also, in the last 100 years gold prices have spiked when fear of inflation and distrust in the economy is high, which given the current economic climate suggests that gold’s value will continue to rise.

Gold has two main disadvantages: The first is that it is expensive and a hassle to store or transport. The second is that it has no passive income; it only has value when you sell it.

While there is a small risk of inflation by a massive gold deposit being found and flooding the market, it is likely that even if a large deposit is found, the company that finds it will restrict the supply to keep the value of gold high, similar to how De Beers kept the price of Diamonds high.

Bitcoin

While I don’t think Bitcoin’s value will ever increase at the rate it did in 2016/17, I do think it will continue to increase slowly and I don’t believe support of it will drop. It also has no risk of inflation. While Cryptocurrencies are more volatile than gold, I don’t think its value will ever crash as badly as it did after the bubble burst in early 2018.

The biggest disadvantage is the risk of losing access to your Bitcoin wallet. While there is a risk of people losing faith in the currency due to potential attacks, I think the risk of it is small, and given the size of the userbase I think even if it was devalued for a while it would eventually recover.

Another disadvantage is its lack of passive income.

NXT

The biggest benefit of NXT is that since it uses proof-of-stake, investing a lot into it will provide a passive income by mining more coins more often, whereas owning a lot of Gold or Bitcoin doesn't help you get more of it (unless you're actively buying and trading well).

The downside of NXT is that its value isn't growing. Trading history shows its value as relatively constant, apart from a short-lived spike just after its creation, and a longer-lived spike during the cryptocurrency bubble of 2017/18. Also given its relatively small size (compared to bitcoin) I believe there's a high risk that any attack on it that would cause people to lose faith in it may cause people to abandon it forever so that it's value never recovers.

Conclusion

While I believe that Bitcoin is likely to provide the best returns on an investment, I am quite risk-averse, so I would probably go with the safer option of investing in Gold. Ideally, I would invest 2/3rds of my wealth in Gold and invest the other 1/3rd in Bitcoin.

Task 4: TRON

The goal of TRON is to help establish a more decentralised Internet by supporting high throughput, high scalability and high availability for Decentralised Apps.

While Bitcoin uses Proof-of-work (POW), TRON uses Delegated Proof of Stake (DPOS) where every 6 hours, 27 Super Representatives (SRs) are elected to mine all blocks until the next vote (The SRs create blocks in a round robin). Any account can run in an election by paying an entrance fee. The top 127 candidates receive a reward relative to the proportion of total votes they received, and the 27 elected SRs also receive 1/27th of the total block reward of all the blocks mined while they were SR. Furthermore, while in power, the committee of 27 SRs can make proposals to change the dynamic network parameters of TRON, and if a proposal receives 19 or more votes it is approved, and the changes are made.

Voters TRON power (vote weight) is calculated by the amount of Tronix (TRX, the cryptocurrency of TRON) they freeze (make unusable for 3 days). Voters may choose SRs based on criteria such as rewards distributed to voters, or by proposals made by SR candidates that the voter believes will increase TRX adoption.

This method of mining creates a block every 3 seconds, and allows a much larger throughput of transactions, with TRON having 2000 Transactions per second (TPS) compared to Bitcoin's 3 TPS.

Another advantage TRON has over Bitcoin is that there are usually no transaction fees. Normal transactions cost bandwidth points, and the number of bandwidth points a transaction costs is equal to the number of transaction bytes. Users can use the 5000 free daily bandwidth points and can freeze TRX to receive more. Alternatively, Users can pay number of bytes * 10 SUN to send a transaction (1 TRX = 1000000 SUN)

TRON transactions are also required to include part of the hash of a recent block header. This prevents the network from Denial of Service, 50%, selfish mining and double spend attacks.

Unlike Bitcoin's script language, which is not Turing Complete, the TRON Virtual Machine (TVM) is forked from Etherium's Virtual machine and is Turing Complete. Additionally, TRON uses TRON Solidarity, a fork of Solidarity which only has the modification of supporting TRX and SUN units.

Unlike Etherium's Gas system, TRON has an Energy model. Energy can be acquired by freezing TRX or by purchasing it directly for 10 SUN = 1 Energy. Energy is required to deploy Smart Contracts, and also to use State-changing functions of smart contracts, but read-only functions execute without energy.

Another Key feature of TRON is its Digital Token Module. Users can customise their own digital token and distribute them at an expense of 1024 TRX. This means that other users can purchase these tokens, which can be used for a variety of things, such as access to content on the creator's website, or access to an event, for example.

As of 21/03/19, TRON is the 10th highest ranking Cryptocurrency with respect to Market Cap, having a Market Cap of $1,497,029,431 and a Volume of $185,552,483 in the last 24 hours. Its value has remained fairly constant, especially since July 2018, which is bad for return of investment, but also means it is not as volatile as other Cryptocurrencies, making it more appealing for day-to-day use.

TRONs source code was released Dec 2017, its testnet launched March 2018 and its mainnet launched in May 2018. Up to this point, they utilised ERC20 Tokens on the Etherium Blockchain, but in June 2018 they Migrated to their own Blockchain, and allowed users to exchange their ERC20 tokens for TRX. Later in June 2018, their Virtual Machine was released, allowing anyone to make DApps for TRON. On 28th February 2019 TRON had a hard-fork to include features such as multi-sig and dynamic energy adjustment relative to real-time network performance. TRON's founder stated that these changes were needed to make TRON institution ready.

The TRON Foundation also acquired BitTorrent and created the BTT token, a token built on the TRON platform, which can be used to buy queue-skips on BitTorrent, allowing leechers to download their file faster, and rewarding seeders for keeping files active on the network for longer. There have been several Airdrop events where TRX holders have been airdropped BTT tokens by the TRON Foundation relative to the amount of TRX they own.

There have been no successful attacks on TRON.

The current highest voted Super Representative is Sesameseed, with 15.6% of votes. It gives 80% of its received rewards back to its community in proportion to votes cast (rewards are given as Seed tokens, paid out weekly, and members can exchange Seed tokens for TRX at any point), 10% is used for operating expenses, and the other 10% is used for funding projects voted on by the community. This has parallels to Bitcoin's mining pools, but whereas members of a bitcoin mining pool must be mining to generate shares to get their part of the reward, there is no real cost to voting for Sesameseed: You freeze your TRX to get your voting power and assign your vote to Sesameseed and that's it. Your vote carries over to the next election unless you change it, so you can be generating Seed tokens without having any of the expenses of mining.

While the concept of Super Representatives initially seems to undermine the whole decentralised purpose of Cryptocurrency, it really isn't much worse than other Cryptocurrencies like Bitcoin where a few large mining pools control the majority of the hash power. Also, the benefits of TRONs DPOS consensus system over Bitcoin's POW consensus are already clear: With the much greater number of Transactions per second, as well as the lack of transaction fees for the majority of transactions and quick confirmation time, I believe that TRON has a much greater chance of widespread everyday adoption than Bitcoin does, and given that TRON has grown to the tenth biggest Cryptocurrency in such a short time-span, it wouldn't surprise me if that widespread adoption came in the next 2 years.